A

Research Proposal

on

"Multifactor and Single Sign-on Authentication in Cloud Computing"

Supervisor

Dr. Anand Sharma
Asst. Professor
CET-MUST
Lakshmangarh, Sikar

Submitted by:

Mr. Rajesh Yadav
En No: 150439

College of Engineering & Technology

Mody University of Science and Technology, Lakshmangarh Sikar,

Rajasthan-332311

CONTENTS

1. Introduction
2. Literature review
3. Research Gap
4. Objective's
5. Approach / Methodology Intended to be Adopted
6. Expected outcome of the proposed Research work
7. Gantt Chart
8. Publications
9. References

Introduction

NIST (National Institute of Standards and Technology) defines cloud computing as follows: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

This definition clearly states that CC helps in minimizing an organization's expenditure towards managing resources and also reduces the burden of maintaining software or hardware by its user. When burden of management, maintaining a software/hardware is reduced, the companies expenditure and time spent towards infrastructure management is reduced and time saved can be utilized in doing some creative work. This is a huge advantage for users/organizations, which not only saves time but also boosts the performance of company by saving time spent on infrastructure.

Benefits of cloud computing

Some common benefits of CC are:

- **Reduced Cost:** Since cloud technology is implemented incrementally (step-by-step), it saves organizations total expenditure.
- **Increased Storage:** When compared to private computer systems, huge amounts of data can be stored than usual.
- **Flexibility:** Compared to traditional computing methods, cloud computing allows an entire organizational segment or portion of it to be outsourced.
- **Greater mobility:** Accessing information, whenever and wherever needed unlike traditional systems (storing data in personal computers and accessing only when near it).
- **Shift of IT focus:** Organizations can focus on innovation (i.e., implementing new products strategies in organization) rather than worrying about maintenance issues such as software updates or computing issues.

Literature Review

The study starts by identifying cloud computing security challenges and their mitigation strategies from the literature. To identify cloud computing security challenges and their solutions, grey literature, systematic literature review etc.

Cloud Computing: Service models

CC can be accessed through a set of services models. These services are designed to exhibit certain characteristics and to satisfy the organizational requirements. From this, a best suited service can be selected and customized for an organization's use. Some of the common distinctions in cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructureas-a-Service (IaaS), Hardware-as-a-Service (HaaS) and Data storage-as-a-Service (DaaS).

Software as a Service (SaaS): The service provider in this context provides capability to use one or more applications running on a cloud infrastructure. These applications can be accessed from various thin client interfaces such as web browsers. A user for this service need not maintain, manage or control the underlying cloud infrastructure (i.e. network, operating systems, storage etc.) [1]. Examples for SaaS cloud's are Salesforce, NetSuite.

Platform as a Service (PaaS): The service provider in this context provides user resources to deploy onto cloud infrastructure, supported applications that are designed or acquired by user. A user using this service has control over deployed applications and application hosting environment, but has no control over infrastructure such as network, storage, servers, operating
systems etc [1]. Examples for PaaS cloud's are Google App Engine, Microsoft Azure, Heroku.

Infrastructure as a Service (IaaS): The consumer is provided with power to control process, manage storage, network and other fundamental computing resources which are helpful to manage arbitrary software and this can include operating system and applications. By using this kind of service, user has control over operating system, storage, deployed applications and possible limited control over selected

networking components [1]. Examples for IaaS cloud's are Eucalyptus (The Eucalyptus Open source Cloud-computing System), Amazon EC2, Rackspace, Nimbus.

Privacy and Anonymization as a Service (PAAS): This service is proposed as a demonstration model to provide data privacy and protection in a particular organization. It also proposes a work-oriented approach to manage data in cloud [2].

Hardware as a Service (HaaS): The idea of buying a hardware or an entire datacenter with a pay-as-you-use scheme which can scale up and down as per user requirements can be termed as Hardware as a Service (HaaS) [2]. Examples for HaaS cloud's are Amazon EC2, IBM's Blue Cloud Project, Nimbus, Eucalyptus, Enomalism [2].

Identity as a Service (IDaaS): This service is targeted for third party service providers who provide Identity and access control functions (including user's life cycle and sign-on process). This can be used in combination with various other services (software, platform or infrastructure services) and also for public and private clouds [3].

Data storage as a Service (DaaS): This service allows user to pay for the amount of data storage he/she is using. With this service there is a separate cloud formed which provides storage as a service [3]. Examples of such kinds of users are Amazon S3, Google Big table, Apache Hbase, etc [2].

Security as a Service (SaaS): This service allows users to create their own security policies and risk frameworks. In this kind of service cloud users must identify, assess, measure and prioritize system risks [4].

Cloud computing: Deployment models

Services can be deployed on one or more deployment models such as, public cloud, private cloud, community cloud and hybrid cloud to use features of cloud computing. Each of these deployment models are explained as follows:

Public cloud: This type of infrastructure is made available to large industrial groups or public. These are maintained and owned by organization selling cloud services [5].

Private cloud: This type of cloud deployment is just kept accessible to the organization that designs it. Private clouds can be managed by third party or the organization itself. In this scenario, cloud servers may or may not exist in the same place where the organization is located [5].

Hybrid cloud: With in this deployment model there can be two or more clouds like private, public or a community. These constituting clouds (combinations of clouds used, such as `private and public', `public and community', etc.) remain different but yet bound together by standardized or preparatory technology that enables application and data portability [5].

Community cloud: This type of cloud infrastructure is shared by several organizations and supports a specific community with shared concerns. This can be managed by an organization or third party and can be deployed or in the organizational premise [5].

Categories of Security Challenges in Cloud Computing

Security considered as the most important subject which should be discussed in the related literature to improve the security of cloud computing application. Main security subjects about cloud computing is as follows:

A. Data Security

Liu [6] believed that cloud computing refers to the quick developments of the users for essay access to the required hardware, software and facilities and other associated capitals in several times. Furthermore, the data security seems to be more important while it is applied for the cloud computing in the SPI background. Cloud computing also faced with several problems, if the experts will not resolve them well, it's fast improvement could be affected too. Data security is common in several

applications and among the associated problems; it can create many problems for the operators while they keep sensitive data in different cloud servers.

1) Availability

Certifying timely and consistent contact for using the related data. An obtainability problem refers to the interruption of contact for using the related data or for the data system [7].

2) Confidentiality

Preserving authorized limitations about the data accessibility and release, like the tools for keeping the individual privacy and exclusive data, a loss of privacy is the illegal disclosure of data [7].

3) Integrity

Guarding against unsuitable data adjustment or destruction and safeguarding the data, non-repudiation and truthfulness, a loss of truthfulness is the unauthorized change or destruction of data [7]. One big problem about the cloud data storage refers to the data integrity confirmation at untrusted servers. As an example, the storage service supplier, that experiences Byzantine problem infrequently, might decide to hide the information errors of the users for their own benefits. The more serious issue is that by saving money and the storage space, the service provider may ignore keeping or deliberately delete the infrequently retrieved information files that belongs to a normal user.

4) Data location

Several regulations for managing the information might vary from country to country. Consequently, transporting confidential information among the countries could be considered as a challenging task. Regarding the cloud setting, the position of the information centers and backups should be understood perfectly to ensure that legal problems wouldn't happen [8].

5) Data Recovery

Data Recovery considered as an important section of each Business Continuity Planning. By applying an unrestricted cloud provider, it should be noted that the Business Continuity Planning and the Data recovery could be expanded to contain catastrophes which affects the public cloud provider. About

natural problems or related disasters, a cloud service provider information center might be inaccessible. About this possibility, it is important to apply a well-thought out disaster retrieval strategy [9].

6) Retention

How long could the personal data which was transported to the cloud retained? Who applies the preservation strategy about the cloud, and how we can manage litigation holds [10].

7) Ownership

Typically, workers or administrations have accessibility to the information and they can manage them well. Once the information moved to the cloud, we have to consider how we can maintain the Information possession [11]. Data ownership refers to the clouded initial move of the cloud, with queries about what happens to information while it moves to the cloud? What occurs while a cloud provider goes out of industry? In addition, what occurs if cloud clients could not pay their bills? [11].

8) Access control

Regarding the cloud setting, the association between capitals and operators considered very commercial hoc and active resource workers and customers are not usually located in a similar security field while clients are typically recognized by their features or qualities, not predefined characteristics.

9) Data lock-in

In the other word, the clients cannot move easily from a SaaS or IaaS vendor to the other one. The client data could be destroyed, that stop users to adopt cloud Computing.

B. Virtual machine level security

Virtual setting contains different VMs, which deliver self-governing security areas. It is hard to manage several VMs effectively, working on a similar physical organization. The most important purpose of Virtualization refers to the way it certifies several VM examples working on a similar physical engine that are separated from each other [12, 13].

1) Hypervisor security

Hypervisor considered as a key software constituent of Virtualization. It usually affects all VMs acts working with the Virtualization host. While an attacker totally controls a hypervisor, then he may apply any activity to the VMs on the host scheme. Two stages in security administration of hypervisor were proposed [1, 9]. Regarding a real hypervisor product, like Xen, OpenVZ or VMware, the attacker usually attempts to exploit the security holes to modify the hypervisor, so that he may install a rootkit on it. The solution is to update and patch the hypervisor product and other virtualization products regularly.

2) Authorization and Authentication

Authorization and Authentication are considered as the most significant features of managing a virtual host reviewing goal. Authorization confirms that clients should be authorized and have consent to do their required tasks. For the authentication, suitable values and existing instruments should be applied to validate related account correctly [14].

3) Networking

Network communications and arrangements are considered as the important security subjects about the cloud computing organizations. Cloud computing embraces cyber infrastructure, and shapes upon periods of investigation in virtualization, dispersed computing, grid computing, utility computing, and more lately, networking, web and software amenities. It usually refers to the service oriented architecture, reduced information technology designed for the users, being more flexible, reduced entire charge of ownership, on request facilities and several other issues [11].

4) Isolation

In the virtual setting of cloud computing, although it reasonably isolated, all VMs have the same hardware and therefore the similar capitals. This might clue to exploit of data leaks and cross-VM attack. For better protection the notion of separation might also be used for better fine-grained properties, like computational capitals, storing and memory [15].

C. application security

Application security refers to the use of system capitals, such as software and hardware for secure requests which holds them in contradiction of malicious saturation that attacks the cloud. Consequently, cloud is usually insecure the application due to the security holes like unconfident software Connectors or APIs interrelating with cloud facilities. There are different threats regarding the security program of the cloud

1) Cloud browser security

In SaaS module Customers computing tasks are allocated to the remote server. The client system is usually applied for the IO take and sends instructions to the cloud. Though there are several security matters in cloud, but browser security is very significant, particularly in cloud computing [16].

2) Cloud malware attack

This kind of attack injects VM malicious or implementation service to cloud computing organization and its goal it is to vary extensively, either stopping, eavesdropping or adapting information by adapting the delicate about overall Capability variations. The aggressive make VM destructive instance of model Implementation Services like, SaaS, IaaS and add it to cloud computing. And its answer refers to the implementation of integrated review, like Services before using it for received desires along the cloud scheme [17].

Research Gap

1. Scalable user authentication model requires key of the manager. If the server fails, the key will not be accessible for authentication.

2. Multi-token authorization connection link carries the completely distributed token that will be hacked and the hacker can access the protected resources.

3. Multi-layer authentication the users will have to enter user information in each section in order to log-in.

4. Single sign-on for authentication & authorization system, is more flexible, reliable and secure, but no private space for any specific service.

Objectives of Propose Research Work

The proposed research work will involve the following points:

1. Implementation of scalable & reliable user authentication for a secure access to cloud environments.

2. Replacement of multi-token authorization & multi-layer authentication through single sign-on in cloud.

3. Implementation of single sign-on authentication with frequency for different services on cloud.

Approach / Methodology Intended To Be Adopted

The proposed work will be conducted on the simulator, CloudSim. It will involve the implementation of.

Objective1. Implementation of scalable & reliable user authentication for a secure access to cloud environments.

We offer an efficient and scalable user authentication scheme for cloud-based environments. In the model uses the concepts of agents, cryptography, and key exchanging to enhance and improve the performance of the user authentication and the rate of scalability in cloud-based environments respectively. For achieving to this purpose, the proposing model will be presenting based on three main agents: first user authentication agent, second user authentication agent and key manager agent. These agents have divided the process of user authentication and managing keys into several parts to improve the rate of efficiency in this process. Furthermore, the suggesting model tries to resist against possible attacks.

Objective2. Replacements of multi-token authorization & multi-layer authentication through single sign-on in cloud.

For using the all types of cloud services gives the single sign-on option. User doesn't require the re-authorization for every service. For this single sign-on we provide high level of security Protocols (i.e. Kerberos, OpenID, etc.).

Objective3. Implementation of single sign-on authentication with frequency for different services on cloud.

In single sign-on authentication for different level of services we provide the multi factor authentication techniques. With the help of this technique we can divide the services in different levels, so we again don't require the re authentication for the same level, but for different level of services we provide another authentication (i.e. biometric, OTP, etc.).

Expected Outcome of Proposed Research Work

The proposed research work will be relevant in the following manner:

- The comparison of existing authentication and authorization protocols and finds the best for applying on new authentication & authorization techniques.
- Improve the user authentication. So only authenticated users can access the services which are allotted to him.
- Multi-token authorization and multi-layer authentication is introduced in single sign-on option.
- Implementation of single sign-on techniques with user trust.

Publication:

1. Rajesh Yadav, Anand Sharma. "Cloud Computing: Data Security Aspect", 3rd International Conference on computing communication, networks and security, at MUST, lakshmangarh Feb, 2018.

Gantt chart

Time		TILL SEP 2018		TILL MAR 2019		TILL OCT 2019
Objectives						
Objective 1						
Objective 2						
Objective 3						

References

[1] Peter Mell and Tim Grance. The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2014.

[2] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu. Cloud computing: a perspective study. New Generation Computing, 28(2):137{146, 2014.

[3] Hutton A. Meisel A. Windel A. Mohammed A. Licciardi A. Seccombe, A. Security guidance for critical areas of focus in cloud computing, v2.1. CloudSecurityAlliance, page 25, 2015. cited By (since 2014).

[4] L.M. Kaufman. Can a trusted environment provide security? Security & Privacy, IEEE, 8(1):50{52, 2013.

[5] T. Dillon, Chen Wu, and E. Chang. Cloud computing: Issues and challenges. In 2015 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pages 27 {33, April 2015.

[6] Liu, X. (2014, January). Data Security in Cloud Computing. In Proceedings of the 2012 International Conference on Cybernetics and Informatics (pp. 801-806). Springer New York.

[7] Winkler, V. (2013a). Chapter 1 - Introduction to Cloud Computing and Security Securing the Cloud (pp. 1-27). Boston: Syngress.

[8] Kumar, P., & Arri, H. S. (2013). Data Location in Cloud Computing. International Journal for Science and Emerging Technologies with Latest Trends, 5(1), 24-27.

[9] Sitaram, D., & Manjunath, G. (2016). Chapter 7 - Designing Cloud Security Moving To The Cloud (pp. 307-328). Boston: Syngress.

[10] Popovic, K., & Hocenski, Z. (2014, May). Cloud computing security issues and challenges. In MIPRO, 2010 proceedings of the 33rd international convention (pp. 344-349). IEEE.

[11] A Vouk, M. (2014). Cloud computing–issues, research and implementations. CIT. Journal of Computing and Information Technology, 16(4), 235-246.

[12] Dorey, P. G., & Leite, A. (2015). Commentary: Cloud computing–A security problem or solution?. information security technical report, 16(3), 89-96.

[13] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2013). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(1), 1-18.

[14] Takabi, H., Joshi, J. B., & Ahn, G. J. (2014). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy, 8(6), 24-31.

[15] You, P., Peng, Y., Liu, W., & Xue, S. (2014, June). Security issues and solutions in cloud computing. In Distributed Computing Systems Workshops (ICDCSW), 2014 32nd International Conference on (pp. 573-577). IEEE.

[16] Google, —Browser security handbook,‖ http://code.google.com/p/browsersec /, 2015.

[17] Subashini, S., & Kavitha, V. (2015). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[18] Seyed Milad Dejamfar* , 2 Sara Najafzadeh (2017). Authentication Techniques in Cloud Computing: A Review.

[19] V. Radhaa, D. Hitha Reddya, Science Direct, December 2012, A Survey on Single Sign-On Techniques.

[20] Lewis, K.D. and Lewis, J.E. (2015). Web Single Sign-On Authentication using SAML. International Journal of Computer Science Issues, IJCSI 2, 41-48